Surveillance
Dell EMC Storage with Digifort Enterprise

Configuration Guide

H15230

REV 1.1

Dell EMC
Surveillance Lab
Tested

digifort

DELLEMC

CONTENTS

CONTENTS

CHAPTER 1

Introduction

This chapter presents the following topics:

Purpose

The purpose of this configuration guide is to help Dell EMC field personnel understand how to configure Dell EMC storage system offerings to simplify the implementation of Digifort Enterprise. This document is not a replacement for the Digifort implementation guide nor is it a replacement for the *Dell EMC Storage with Digifort Enterprise: Sizing Guide*.

Digifort Enterprise provides a comprehensive system for video surveillance. This system enables customers' network and security teams to collaborate effectively in a highly scalable environment, combining both video and network techniques to optimize performance. The Dell EMC storage system provides no single point of failure, while the SEnterprise design ensures resilience.

Use this guide to determine the requirements for a successful Digifort Enterprise installation and storage-specific configuration requirements.

Digifort Enterprise comprises all of the features available in the Digifort System, offering total management of unlimited cameras and alarm devices. Digifort Enterprise is ideal for any company that wants total control of its security project, to ensure high performance, reliability, and scalability. Enterprise enables the use of several models of IP cameras and video servers from various manufacturers, which allows you to choose hardware that best meets the client's needs.

Scope

This guide is intended for internal Dell EMC personnel and qualified Dell EMC and Digifort partners. It provides configuration instructions for installing the Digifort Enterprise video management software using Dell EMC storage platforms.

The following Dell EMC storage systems have been tested:

- EMC VNX™
- EMC VNXe™
- EMC VSS™

This guide supplements the standard *EMC VNX Storage Best Practices with Video Management Systems: Configuration Guide* and provides configuration information specific to Digifort Enterprise.

Note

All performance data in this guide was obtained in a rigorously controlled environment. Performance varies depending on the specific hardware and software used.

Assumptions

This solution assumes that internal Dell EMC personnel and qualified Dell EMC partners are using this guide with an established architecture.

This guide assumes that the Dell EMC partners who intend to deploy this solution are:

- Associated with product implementation
- Digifort-certified to install Digifort Enterprise services
- Proficient in installing and configuring VNX/VNXe storage solutions

- Familiar with installing and configuring VMware hypervisors and the appropriate operating system, such as Microsoft Windows or a Linux distribution

- Able to access the *EMC VNX Storage with Video Management Systems: Configuration Guide*

The configurations that are documented in this guide are based on tests that we conducted in the Dell EMC Surveillance Lab using worst-case scenarios to establish a performance baseline. Lab results might differ from individual production implementations.

CHAPTER 2

Configuring the solution

This chapter presents the following topics:

Design concepts

There are many design options for a Digifort Enterprise implementation. Digifort offers many training courses related to design and implementation. These design details are beyond the scope of this paper.

The *Digifort Enterprise Manual Administration Client Version 7.1.0.0* provides the information that you need to plan a Enterprise VMS system.

These guides are intended for systems integrators and architects, network IT planners, and system administrators. These guides assume that readers know what Digifort Enterprise Video Management Software (VMS) does and how it works, and know how to deploy and configure Windows IP networks. These documents are available from a Digifort partner or through the Digifort Partner network.

In the *Digifort Enterprise Manual Administration Client Version 7.1.0.0*, Digifort recommends a segregated implementation. A common segregated implementation example could consist of a user network, a camera network, and a storage network. Other considerations covered in the planning guide include multicast, third-party software, ports used by Enterprise, and other important information. This white paper is not intended to replace or supersede any Digifort document.

The following figure represents the basic configuration that was tested in our lab.

Figure 1 Digifort Enterprise architecture
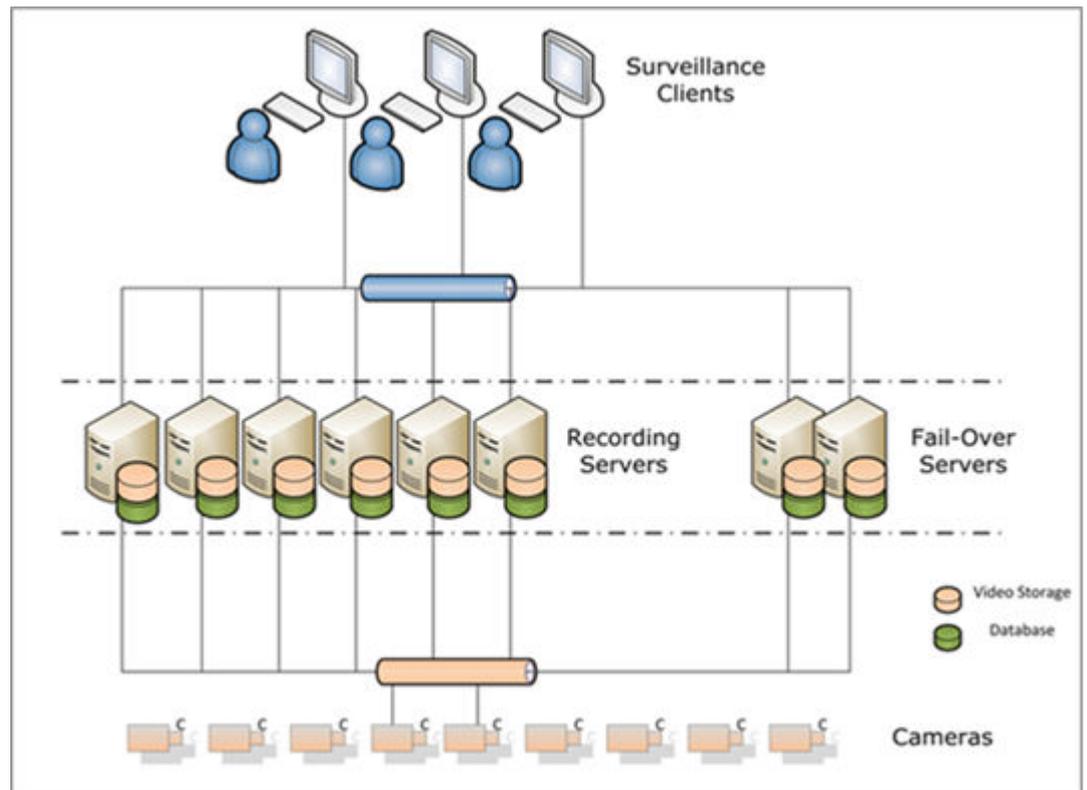
EMC VNX

VNX storage is ideal for recording and managing terabytes of video from distributed locations. This section describes best practices for configuring a VNX or VNXe storage system for this solution.

The VNX family includes the VNX, VNXe, and VNX-VSS series arrays. The VNXe series is designed for small to midsize environments. The VNX series is designed for midtier to enterprise storage environments, is ideal for distributed environments, and can scale to handle large petabyte (PB) environments with block-only requirements at central locations.

Disk drives

Although any supported drive will work, video surveillance systems typically rely on the density of the array. Dell EMC recommends NL-SAS drives of the highest available density in this solution. In general, we used one-terabyte (TB) or multi-TB NL-SAS drives when performing our tests.

Note

Because of the high percentage of sequential, large block writes, Dell EMC does not recommend using flash drives for video storage within a surveillance application.

Storage pool configuration (recommended)

The tests we conducted show how storage pools that are defined with the maximum allowable number of disks per pool perform as well as, or better than, traditional RAID groups. Therefore, Dell EMC recommends that you use storage pools rather than RAID groups. Storage pools also reduce the required array management tasks.

The VNX family array architecture is optimized for storage pools. A storage pool is a construct that is built over one, or more commonly multiple, RAID groups. LUNs are built on top of the storage pool. The read/write activity is a random distribution across all disks defined to the storage pool. This distribution results in increased and balanced per disk utilization and improved performance when compared to traditional RAID implementations.

The RAID groups underlying storage pools can be either RAID 5 or RAID 6. The default and recommended RAID configuration for a VNXe or VSS1600 array using NL-SAS drives is RAID 6. Either RAID 5 or RAID 6 can be used with VNX arrays. RAID 5 is used for optimizing the array to achieve the maximum amount of storage and RAID 6 is used for enhancing data protection. Our tests using an isolated surveillance infrastructure did not reveal any notable performance variances when using RAID 5 as compared to RAID 6.

Building a storage pool is a straightforward process. You can configure either RAID 5 or RAID 6 pools depending on the VNX or VNXe storage system restrictions and the level of risk that the customer is willing to accept. When configuring storage pools, use large storage pools with large logical unit number (LUN) sizes, and configure the LUNs as thick. Do not use thin LUN provisioning.

Dell EMC recommends the following RAID configurations for VNX arrays:

- RAID 5 or RAID 10 with SAS drives
- RAID 6 with NL-SAS drives

Procedure

1. In Unisphere, select **Storage** > **Storage Pools** for block.
2. Click **Create** under **Pools** in the **Pools** section.
3. Set the following options for the storage pool:
   - Storage pool name
   - RAID type
   - Number of SAS drives
   - Number of NL SAS drives

4. Choose a method for selecting disks to include in the storage pool:
   - **Automatic**: Provides a list of available disks.
   - **Manual**: Enables you to select specific disks to include in the storage pool from a list of available disks. Be sure to clear the automatic disk recommendation list before you select new disks from the list.
5. Select **Perform a Background verify on the new storage** and set the priority to medium.
6. Click **Apply**, and then click **YES** to create the storage pool.

LUN configuration

A VNX pool LUN is similar to a classic LUN. Pool LUNs comprise a collection of slices. A slice is a unit of capacity that is allocated from the private RAID groups to the pool LUN when it needs additional storage. Pool LUNs can be thin or thick.

Thin LUNs typically have lower performance than thick LUNs because of the indirect addressing. The mapping overhead for a thick LUN is less than for a thin LUN.

Thick LUNs have more predictable performance than thin LUNs because they assign slice allocation at creation. Because thick LUNs do not provide the flexibility of oversubscribing like a thin LUN, use thick LUNs for applications where performance is more important than saving space.

Thick and thin LUNs can share the same pool, enabling them to have the same ease-of-use and benefits of pool-based provisioning.

Procedure

1. In Unisphere, right-click a storage pool and then click **Create LUN**.
2. Type the user capacity for the LUN.
3. Type the starting **LUN ID**, and then select the number of LUNs to create.

   For example, if the selected LUN ID is 50, and the selected number of LUNs to create is 3, the names for the LUNs are 50, 51, and 52.
4. Select **Automatically assign LUN IDs as LUN names**.
5. Click **Apply**.

Fibre Channel configuration

To transfer traffic from the host servers to shared storage, the serial-attached network (SAN) uses the Fibre Channel (FC) protocol that packages SCSI commands into FC frames.

Note

iSCSI is prevalent for video security implementations because it often provides a lower-cost option when compared to FC.

To restrict server access to storage arrays that are not allocated to the server, the SAN uses zoning. Typically, zones are created for each group of servers that access a shared group of storage devices and LUNs. A zone defines which HBAs can connect to specific service providers (SPs). Devices outside a zone are not visible to the devices inside the zone.

Zoning is similar to LUN masking, which is commonly used for permission management. LUN masking is a process that makes a LUN available to some hosts and unavailable to other hosts.

Zoning provides access control in the SAN topology. Zoning defines which HBAs can connect to specific targets. When you use zoning to configure a SAN, the devices outside a zone are not visible to the devices inside the zone.

Zoning has the following effects:

- Reduces the number of targets and LUNs presented to a host
- Controls and isolates paths in a fabric
- Prevents non-ESXi systems from accessing a particular storage system and from possible virtual machine file system (VMFS) data loss
- Optionally, separates different environments, such as test and production environments

With VMware ESXi hosts, use single-initiator zoning or single-initiator-single-target zoning. The latter is the preferred zoning practice because it is more restrictive and prevents problems and misconfigurations that can occur on the SAN.

Dell EMC PowerPath

Dell EMC PowerPath™ is recommended for block storage (FC and iSCSI) implementations. PowerPath Multipathing automates data path management, failover and recovery, and optimizes load balancing to ensure application availability and performance.

FC LUN configuration for a virtualized environment

Fibre Channel LUNs can be configured using two methods for virtualized environments.

Raw device mappings (RDM)

RDM can be used for virtual machine archivers to store Video data. The RDM allows a virtual machine to access and use the storage device directly. The RDM contains metadata for managing and redirecting disk access to the physical device. The file gives you some of the advantages of direct access to a physical device while keeping some advantages of a virtual disk in VMFS. As a result, it merges VMFS manageability with raw device access.

FC datastores

ESXi uses datastores, which are logical containers that hide specifics of physical storage from virtual machines and provide a uniform model for storing virtual machine files. Datastores that you deploy on block storage devices use the vSphere VMFS format, a special high-performance file system format that is optimized for storing virtual machines.

iSCSI initiators

Software or hardware initiators may be used with VMware ESXi server or a non-virtualized server.

Microsoft Internet SCSI (iSCSI) initiators

For both physical servers and VMware ESXi server, the Dell EMC Surveillance Lab uses Microsoft iSCSI initiators with excellent results.

Hardware iSCSI initiators

Hardware iSCSI initiators can be used. There are many iSCSI initiators available on the market, and results might vary.

VNXe RAID configuration

VNXe offers RAID 5, RAID 6, and RAID 10 configurations. Different configurations offer different types of protection against disk failures.

Dell EMC recommends the following RAID configurations:

- RAID 5 or RAID 10 with SAS drives
- RAID 6 with NL-SAS drives

Recommended cache configuration

EMC VNX generation 2 systems, such as VNX5200 or VNX5400, manage the cache. If the array is shared with other applications, you can use a lower write cache value, but avoid excessive forced flushes.

Dell EMC recommends that you configure the cache as 90 percent write and 10 percent read if the storage array does not automatically adapt to the write characteristics of video surveillance (for example, EMC VNX5500 or EMC VNX-VSS100).

Releases tested

The following tables list the firmware builds and software releases used for our tests.

Table 1 Firmware builds

Model	Firmware
VNXe1600	VNXe OE 3.1.3.7141854
VSS1600	VNX OE 3.1.3.7141854

Table 2 Digifort Enterprise releases

Release	Subrelease
Digifort Enterprise	7.1.0.0

VMware ESXi requirements and recommendations

During all the tests, we assumed that the vCPU, memory, and network were configured correctly according to Digifort's best practices to operate within Enterprise parameters.

The following virtual machine configuration was used for all tests:

- vCPUs (virtual CPUs): 8
- vMemory (virtual memory): 12 GB
- Network Driver: Vmxnet3 with 10 GbE
- Disk Driver: SCSI

This document assumes that the person that performs the configuration is familiar with these basic configuration activities.

CHAPTER 3

Conclusion

This chapter presents the following topics:

Summary

Dell EMC performed comprehensive testing with Digifort Enterprise against many EMC VNX and VNXe arrays.

Depending on the implementation needs, you can use Dell EMC storage for Digifort Enterprise.

The Digifort architecture and product suite allows extreme scaling, from a few cameras to up to tens of thousands of cameras, by using Dell EMC storage.

EMC VNX

Compared to traditional block-level storage, the use of storage pools to create LUNs within the VNX arrays greatly simplifies the configuration and increases the performance. Either iSCSI or FC can be implemented. FC performs better than iSCSI.

EMC VSS

The VNX Video Surveillance Storage (VSS) is a storage solution that is purpose-built to meet the unique demands of the video surveillance environment. We found that this high-availability, low-cost array performs comparably to other arrays in the VNX family.

EMC VNXe

An iSCSI-connected VNXe array, implemented with storage pools, provides a cost-effective implementation while maintaining the expected performance. Many mid-sized deployments can use VNXe.